Controls and compliance checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☐	☑	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☑	Only authorized users have access to customers’ credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers’ data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice

☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☑	☐	Data is available to individuals authorized to access it.

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

**Potential solutions to have Botium Toys in alignment with National and International data security compliance and regulations are as follows:*

- *Review each internal position's roles and responsibilities, then group into teams. Each team will have specific duties pertaining to a particular area of the business. Each access privilege must be tailored to each group's specific area of responsibility. If more access is needed, users can request additional privileges via an IT ticket with supporting evidence of why the access is needed. Then, IT Management can review and approve/deny on a case-by-case basis*
- *Create and implement disaster recovery plans or outsource to have them created for the business.*
- *There are password policies in place; however, they need to be revised to increase the minimum level of security in addition to a mandatory password change once per quarter.*
- *Purchase and install enterprise level intrusion detection system (IDS) and assign the role of monitoring this software to a specific team.*
- *The use of backups was not described in the risk assessment. In case backups are not available, create a backup procedure that mandates and automates a daily or weekly system backup - this backup data can be used in the aforementioned disaster recovery plan.*
- *Add to the existing procedure, if available, or create a procedure that includes the scheduled monitoring and maintenance of legacy systems.*

- *Install and/or implement an encryption procedure that safeguards all data in Botium's intranet, with a specific focus on customer financial records.*
- *Install an enterprise level password manager that all employees will be mandated to use. Choose a password manager that allows for secure password generation that will meet the new requirements of the updated password policy (once complete).*